

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-342292
 (43)Date of publication of application : 29.11.2002

(51)Int.Cl. G06F 15/00
 G06F 12/14
 G06F 17/30
 G06F 17/60

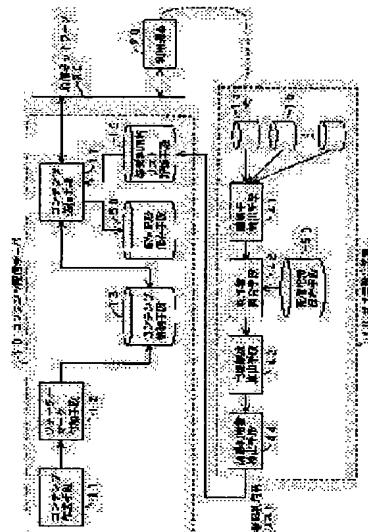
(21)Application number : 2001-147746 (71)Applicant : SONY CORP
 (22)Date of filing : 17.05.2001 (72)Inventor : ISHII HIDEHIRO

(54) CONTENTS DELIVERY SERVER AND DETECTION DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To estimate or specify a user or equipment used which are related to illegal copying.

SOLUTION: When a contents delivery request is issued from a user via a communication network 30, a contents transmitting means 17 authenticates the user, and at determining that the user is listed up as a suspected user, by referring to a suspicious users list storage means 19, transmits duplicated contents exclusive of the user added with a watermark, including a user identifier for identifying the user. When the user is not listed as being a suspected user, the contents transmitting means 17 transmits duplicated contents added with a watermark including a proper duplication identifier, and records a user identifier for identifying the user and the duplication identifier added to the transmitted duplicated contents as a pair in a distribution record preserving means 50.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

[What is claimed is:]

[Claim 1]

A contents server comprising:

an identifier adding section that adds a user identifier, which identifies a user, who uses a content, or a utilization device identifier, which identifies a device, to contents corresponding to content data or a computer program; and

a content transmission section that transmits the content with the user identifier or the utilization device identifier added.

[Claim 2]

A contents server comprising:

an identifier adding section that adds replication identifiers, each which identifies each of multiple replicated contents, to the multiple replicated contents corresponding to content data or computer programs;

a content transmission section that transmits the replicated content with the replication identifier added; and

a distribution record storage section that records, as a pair, a user identifier, which identifies a user as a destination of the replicated content, or a utilization device identifier, which identifies a utilization device, and the replication identifier added to the replicated content.

[0011]

[Embodiment of the Invention]

[First embodiment ... FIG.1]

FIG.1 shows a first embodiment of a content distribution system of this invention.

[0012]

The content distribution system of this invention is composed of a content distribution server 10 on a content distribution side, a utilization device 20 on a user side, a communication network 30 such as the Internet that performs communication between the content distribution server 10 and the utilization device 20, and a user

detection device 40 on the content distribution side.

[0013]

In the first embodiment, the content distribution server 10 includes a content creation section 11, a content storage section 13, a watermark adding section 15, and a content transmission section 17, and the user detection device 40 includes an identifier extraction section 41.

[0014]

The content created by the content creation section 11 of the content distribution server 10, that is, data or a computer program such as image software, music software, game software, etc., is stored in the content storage section 13. It should be noted that the content creation section 11 does not always have to be provided in the content distribution server 10, and content may be created by an external unit of the content distribution server 10 and the created content may be stored in the content storage section 13 in the content distribution server 10.

[0015]

Upon reception of a content distribution request from a user (utilization device 20) via the communication network 30, the content transmission section 17 authenticates the user, reads the content requested by the user from the content storage section 13, adds a watermark, which includes a user identifier that identifies the user, to the content using the watermark adding section 15, and transmits the resultant content to the user.

[0016]

The utilization device 20 is an information terminal, such as a personal computer, PDA (Personal Digital Assistants), a cellular phone, etc., that receives distributed content, downloads the distributed content, and processes the downloaded content. If the distributed content is image software or music software, the utilization device 20 displays the image on a display and outputs music from a speaker, an earphone, etc. If the distributed content is game software, the user can play a game using the utilization device 20.

[0017]

There is a possibility that the content downloaded to the utilization device 20 will be illegally copied. However, when a person, who will protect a right of content, finds out content having suspicion of an illegal copy, he/she can specify a user, who is suspected of making an illegal copy, using the user detection device 40.

[0018]

In other words, the user detection device 40 specifies the user, who is suspected of making an illegal copy, by extracting a user identifier from content 1 having suspicion of an illegal copy, which will be recorded on a recording medium and transmitted, using an identifier extraction section 41.

[0019]

As mentioned above, according to this embodiment, it is possible to specify the user, who is suspected of making an illegal copy. Unlike the conventional method in which a watermark is added to content in reproducing the content by a reproduction device, this embodiment can specify the user, who is suspected of making an illegal copy, even when a key for using the content is illegally obtained or a copyright protection function of the utilization device 20 is nullified.

[0020]

(Other examples)

The aforementioned example shows the case in which the user, who made a request for content distribution, is authenticated and the watermark, which includes the user identifier that identifies the relevant user, is added to the content. However, the utilization device 20, which made a request for content distribution, is authenticated and the watermark, which includes the utilization device identifier that identifies the relevant utilization device 20, may be added to the content.

[0021]

Moreover, the content transmission section 17 may be configured in such a way that the watermark, which includes the user identifier or utilization device identifier, is added to content without performing explicit authentication by the watermark adding

section 15 and the content is coded to be decoded with a key that the relevant user possesses, and the result is transmitted to the relevant user.

[0022]

Still moreover, the user identifier or utilization device identifier may be added as a header instead of the watermark, with a coded message or a plain text. However, in this case, if a user, who will make an illegal copy, has some degree of technique, there is a possibility that the user identifier or the utilization device identifier will be deleted on copying. In view of this point, it is preferable that the content be added as the watermark as in the aforementioned example.

[0023]

[Second embodiment ... FIG.2]

FIG.2 shows a second embodiment of a content distribution system of this invention.

[0024]

The content distribution system is the same as that of the first embodiment in terms of the point that the system is composed of the content distribution server 10, the utilization device 20, the communication network 30 and the user detection device 40.

[0025]

In the second embodiment, the content distribution server 10 includes a content creation section 11, a content storage section 13, a content transmission section 17, and a distribution record storage section 50, and the user detection device 40 includes an identifier extraction section 41, a user collation section 42, and a distribution record storage section 50. The distribution record storage section 50 is shared with the content distribution server 10 and the user detection device 40.

[0026]

In this embodiment, each content is replicated into multiple contents by the content creation section 11 of the content distribution server 10, content replication identifiers, which identifies with each other, are allocated to the respective replicated contents, and the watermarks, each including the

replication identifier, are added thereto by the watermark adding section 12, and the respective replicated contents are stored in the content storage section 13. It is preferable that no overlap of replication identifiers occur.

[0027]

Upon reception of a content distribution request from a user via the communication network 30, the content transmission section 17 authenticates the user, selects a replication of the content, which is requested by the user and which has an appropriate replication identifier added and reads the selected content from the content storage section 13. Then, the resultant content is transmitted to the user. At the same time, the replication identifier added to the replicated content and the user identifier, which identifies the relevant user, are recorded, as a pair, on the distribution record storage section 50. The replication identifier may be selected, for example, at random.

[0028]

In the user detection device 40, a user, who will protect the right of content, extracts a replication identifier from content 1 with suspicion of an illegal copy, which will be recorded on a recording medium and transmitted, using the identifier extraction section 41. Moreover, the user refers to the distribution record in the distribution record storage section 50 based on the replication identifier using the user collation section 42, and detects a user identifier, which identifies a user (one or multiple users), to which the replicated content with the replication identifier added was distributed, using the user detection device 40.

[0029]

Therefore, according to this embodiment, it is possible to detect a user, who is suspected of making an illegal copy, and to specify the user. Furthermore, in this embodiment, the replication identifier is selected at random and the replicated contents with the replication identifier added thereto may be transmitted to the user at the content distribution time, resulting in a reduced load of the content distribution server 10 as compared with that of the

first embodiment.

FIG. 2

10: CONTENT DISTRIBUTION SERVER
11: CONTENT CREATION SECTION
12: WATERMARK ADDING SECTION
13: CONTENT STORAGE SECTION
17: CONTENT TRANSMISSION SECTION
20: USER DEVICE
30: COMMUNICATION NETWORK
50: DISTRIBUTION RECORD STORAGE SECTION

40: USER DETECTION DEVICE
41: IDENTIFIER EXTRACTION SECTION
42: USER COLLATION SECTION
USER IDENTIFIER

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2002-342292

(P2002-342292A)

(43)公開日 平成14年11月29日 (2002.11.29)

(51)Int.Cl. ⁷	識別記号	F I	テマコード(参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 Z 5 B 0 1 7
12/14	3 2 0	12/14	3 2 0 E 5 B 0 7 5
17/30	1 2 0	17/30	1 2 0 A 5 B 0 8 5
17/60	1 4 2	17/60	1 4 2

審査請求 未請求 請求項の数 8 O.L. (全 8 頁)

(21)出願番号 特願2001-147746(P2001-147746)

(22)出願日 平成13年5月17日 (2001.5.17)

(71)出願人 000002185
ソニー株式会社
東京都品川区北品川6丁目7番35号

(72)発明者 石井 秀浩
東京都品川区北品川6丁目7番35号 ソニ
一株式会社内

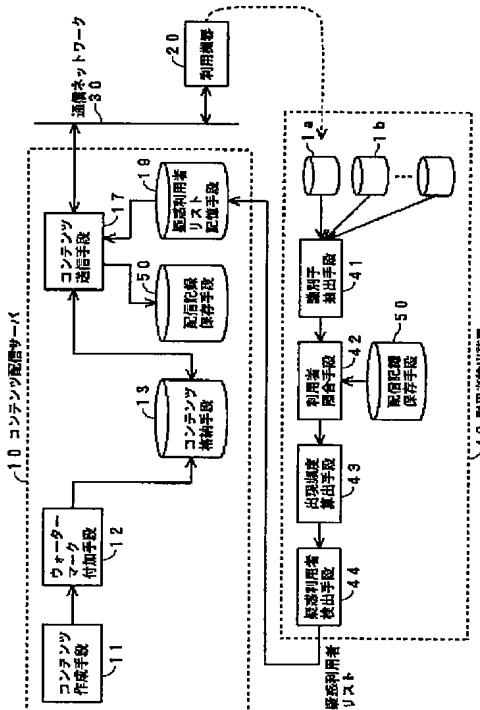
(74)代理人 100091546
弁理士 佐藤 正美
Fターム(参考) 5B017 AA06 BA09 CA15 CA16
5B075 KK54 KK68 NK21 PR04
5B085 AE02 AE04 AE29 BG07

(54)【発明の名称】 コンテンツ配信サーバおよび検出装置

(57)【要約】

【課題】 不正コピーに関与した利用者または利用機器を推定または特定できるようにする。

【解決手段】 通信ネットワーク30を介して利用者からコンテンツ配信要求があったとき、コンテンツ送信手段17は、当該利用者を認証し、疑惑利用者リスト記憶手段19を参照して、当該利用者が疑惑利用者としてリストアップされているときには、当該利用者を識別する利用者識別子を含むウォーターマークが付加された、当該利用者の専用の複製コンテンツを送信する。当該利用者が疑惑利用者としてリストアップされていないときは、適当な複製識別子を含むウォーターマークが付加された複製コンテンツを送信するとともに、当該利用者を識別する利用者識別子と、送信した複製コンテンツに付加された複製識別子とを、組として配信記録保存手段50に記録する。



【特許請求の範囲】

【請求項1】ある内容のデータまたはコンピュータプログラムであるコンテンツに、そのコンテンツを利用する者または機器を識別する利用者識別子または利用機器識別子を付加する識別子付加手段と、
その利用者識別子または利用機器識別子が付加されたコンテンツを送信するコンテンツ送信手段と、
を備えるコンテンツ配信サーバ。

【請求項2】ある内容のデータまたはコンピュータプログラムであるコンテンツの複数の複製に、それぞれの複製コンテンツを識別する複製識別子を付加する識別子付加手段と、
その複製識別子が付加された複製コンテンツを送信するコンテンツ送信手段と、
その複製コンテンツの送信先の利用者または利用機器を識別する利用者識別子または利用機器識別子と、その複製コンテンツに付加された複製識別子とが、組として記録される配信記録保存手段と、
を備えるコンテンツ配信サーバ。

【請求項3】請求項2のコンテンツ配信サーバにおいて、
コンテンツの不正コピーに関与した疑いのある利用者または利用機器を識別する利用者識別子または利用機器識別子が、疑惑利用者または疑惑利用機器として記録される記憶手段を備え、

前記コンテンツ送信手段は、前記記憶手段に疑惑利用者または疑惑利用機器として記録されている利用者または利用機器に複製コンテンツを送信するときには、当該の利用者または利用機器を識別する利用者識別子または利用機器識別子が付加された複製コンテンツを送信するコンテンツ配信サーバ。

【請求項4】請求項1～3のいずれかのコンテンツ配信サーバにおいて、

前記識別子付加手段は、前記利用者識別子または利用機器識別子、または前記複製識別子を、ウォーターマークとして、前記コンテンツまたは前記複製コンテンツに付加するコンテンツ配信サーバ。

【請求項5】ある内容のデータまたはコンピュータプログラムであるコンテンツのコピーから、そのコピーの元になったコンテンツの配信先の利用者または利用機器を識別する利用者識別子または利用機器識別子を抽出する識別子抽出手段を備える検出装置。

【請求項6】ある内容のデータまたはコンピュータプログラムであるコンテンツのコピーから、そのコピーの元になったコンテンツの配信時に当該コンテンツに付加された識別子を抽出する識別子抽出手段と、
配信されたコンテンツに付加された識別子と、当該コンテンツの配信先の利用者または利用機器を識別する利用者識別子または利用機器識別子とが、組として記録される配信記録保存手段と、

前記識別子抽出手段によって抽出された識別子によって、前記配信記録保存手段の記録内容を参照して、前記コピーの元になったコンテンツの配信先の利用者または利用機器を検出する照合手段と、
を備える検出装置。

【請求項7】請求項6の検出装置において、
前記照合手段によって検出された利用者または利用機器の出現頻度を算出する出現頻度算出手段を備える検出装置。

10 【請求項8】請求項7の検出装置において、
前記出現頻度算出手段の出力から、出現頻度が所定値以上の利用者または利用機器を、コンテンツの不正コピーに関与した疑いのある利用者または利用機器として検出する検出手段を備える検出装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、コンテンツを配信するサーバ、およびコンテンツのコピーからコンテンツの不正コピーに関与した疑いのある利用者または利用機器を検出する装置に関する。

20 【0002】なお、この発明では、画像ソフト、音楽ソフト、ゲームソフトなど、ある内容のデータまたはコンピュータプログラムを、コンテンツと定義する。

【0003】

【従来の技術】画像ソフト、音楽ソフト、ゲームソフトなどのコンテンツについては、法律上の権利を持たない者または方法による不正利用、特に不正コピーが、問題となっている。

30 【0004】コンテンツの不正コピーを防止し、著作権を保護するために、従来、コンテンツの暗号化やtamper-resistance技術が考えられており、また再生機器でコンテンツを再生する際に、利用者や再生機器を識別する識別子を含むウォーターマークをコンテンツに付加する方法が考えられている。

【0005】前者の、暗号化やtamper-resistance技術によれば、コンテンツの不正コピーを、ある程度防止することができ、後者の、再生時に利用者識別子または再生機器識別子を含むウォーターマークをコンテンツに付加する方法によれば、再生出力からコンテンツが不正にコピーされた場合に、不正コピーに関与した利用者または再生機器を検出することができる。

【0006】

【発明が解決しようとする課題】しかしながら、前者の、暗号化やtamper-resistance技術による方法では、暗号アルゴリズムに対する攻撃、brute-force attackまたはsocial engineeringなどによる暗号鍵の入手、またはtamper-resistance技術に対する攻撃などによって、コンテンツが不正にコピーされてしま

まうことがある。

【0007】また後者の、再生時に利用者識別子または再生機器識別子を含むウォーターマークをコンテンツに付加する方法では、何らかの方法によって、ウォーターマークを付加する前のコンテンツが不正にコピーされた場合や、コンテンツ利用のための鍵が不正に入手された場合には、不正コピーに関与した利用者または再生機器を検出することができない。

【0008】そこで、この発明は、コンテンツを配信する場合に、利用者側でコンテンツが不正にコピーされたとき、不正コピーに関与した利用者または利用機器を推定または特定することができるようとしたものである。

【0009】

【課題を解決するための手段】この発明のコンテンツ配信サーバは、ある内容のデータまたはコンピュータプログラムであるコンテンツに、そのコンテンツを利用する者または機器を識別する利用者識別子または利用機器識別子を付加する識別子付加手段と、その利用者識別子または利用機器識別子が付加されたコンテンツを送信するコンテンツ送信手段と、を備えるものとする。

【0010】上記の構成のコンテンツ配信サーバでは、利用者側でコンテンツが不正にコピーされた場合、コンテンツの権利を保護しようとする者は、そのコピー入手して、それから利用者識別子または利用機器識別子を抽出することによって、不正コピーに関与した利用者または利用機器を特定することができる。

【0011】

【発明の実施の形態】【第1の実施形態…図1】図1は、この発明のコンテンツ配信システムの第1の実施形態を示す。

【0012】この発明のコンテンツ配信システムは、コンテンツ配信側のコンテンツ配信サーバ10、利用者側の利用機器20、コンテンツ配信サーバ10と利用機器20との間で通信を行うインターネットなどの通信ネットワーク30、およびコンテンツ配信側の利用者検出装置40によって構成される。

【0013】第1の実施形態では、コンテンツ配信サーバ10は、コンテンツ作成手段11、コンテンツ格納手段13、ウォーターマーク付加手段15、およびコンテンツ送信手段17によって構成し、利用者検出装置40は、識別子抽出手段41によって構成する。

【0014】コンテンツ配信サーバ10のコンテンツ作成手段11で作成されたコンテンツ、すなわち、画像ソフト、音楽ソフト、ゲームソフトなどのデータまたはコンピュータプログラムは、コンテンツ格納手段13に格納される。ただし、コンテンツ作成手段11は、必ずしもコンテンツ配信サーバ10内に設けられる必要はなく、コンテンツ配信サーバ10の外部でコンテンツが作成され、その作成されたコンテンツがコンテンツ配信サーバ10内のコンテンツ格納手段13に格納される構成

としてもよい。

【0015】コンテンツ送信手段17は、通信ネットワーク30を介して利用者（利用機器20）からコンテンツ配信要求があったとき、当該利用者を認証して、コンテンツ格納手段13から、当該利用者が要求するコンテンツを読み出し、ウォーターマーク付加手段15によって、そのコンテンツに当該利用者を識別する利用者識別子を含むウォーターマークを付加して、そのコンテンツを、当該利用者に送信する。

【0016】利用機器20は、パソコンコンピュータ、PDA（Personal Digital Assistants）、携帯電話機など、配信されたコンテンツを受信し、取り込んで（ダウンロードして）、処理する情報端末であって、配信されたコンテンツが画像ソフトや音楽ソフトであれば、その画像をディスプレイ上に表示し、音楽をスピーカやイヤホンなどから出力することができるものであり、配信されたコンテンツがゲームソフトであれば、それによってゲームを行うことができるものである。

【0017】利用機器20に取り込まれたコンテンツは、不正にコピーされる可能性がある。しかし、コンテンツの権利を保護しようとする者は、不正コピーの疑いのあるコンテンツを発見したら、利用者検出装置40によって、不正コピーの疑いのある利用者を特定することができる。

【0018】すなわち、利用者検出装置40では、識別子抽出手段41によって、記録媒体に記録されるなどによって伝送される、不正コピーの疑いのあるコンテンツ1から、利用者識別子を取り出すことによって、不正コピーの疑いのある利用者を特定する。

【0019】以上のように、この実施形態によれば、不正コピーの疑いのある利用者を特定することができる。再生機器でコンテンツを再生する際にコンテンツにウォーターマークを付加する従来の方法とは異なり、この実施形態によれば、コンテンツ利用のための鍵が不正に入手された場合や、利用機器20の著作権保護機能が無効化された場合でも、不正コピーの疑いのある利用者を特定することができる。

【0020】（他の例）上述した例は、コンテンツ配信要求をした利用者を認証して、当該利用者を識別する利用者識別子を含むウォーターマークをコンテンツに付加する場合であるが、コンテンツ配信要求をした利用機器20を認証して、当該利用機器20を識別する利用機器識別子を含むウォーターマークをコンテンツに付加してもよい。

【0021】また、コンテンツ送信手段17では、明示的な認証を行わずに、ウォーターマーク付加手段15によって、コンテンツに利用者識別子または利用機器識別子を含むウォーターマークを付加し、さらに、そのコンテンツを、当該利用者が所有する鍵で復号できるように

暗号化して、当該利用者に送信するように構成してもよい。

【0022】さらに、利用者識別子または利用機器識別子を、ウォーターマークとして付加しないで、ヘッダとして平文または暗号文で付加してもよい。ただし、この場合には、不正コピーをしようとする者が、ある程度の技術を持っていると、コピーの際、利用者識別子または利用機器識別子が削除されてしまう可能性がある。その点で、上述した例のようにウォーターマークとして付加する方が好ましい。

【0023】【第2の実施形態…図2】図2は、この発明のコンテンツ配信システムの第2の実施形態を示す。

【0024】コンテンツ配信システムが、コンテンツ配信サーバ10、利用機器20、通信ネットワーク30、および利用者検出装置40によって構成される点は、第1の実施形態と同じである。

【0025】第2の実施形態では、コンテンツ配信サーバ10は、コンテンツ作成手段11、ウォーターマーク付加手段12、コンテンツ格納手段13、コンテンツ送信手段17、および配信記録保存手段50によって構成し、利用者検出装置40は、識別子抽出手段41、利用者照合手段42、および配信記録保存手段50によって構成する。配信記録保存手段50は、コンテンツ配信サーバ10と利用者検出装置40で共用する。

【0026】この実施形態では、コンテンツ配信サーバ10のコンテンツ作成手段11で、各コンテンツが複数に複製され、ウォーターマーク付加手段12で、その各複製コンテンツに、互いを識別する複製識別子が割り当てられ、複製識別子を含むウォーターマークが付加されて、その各複製コンテンツが、コンテンツ格納手段13に格納される。複製識別子は一切重複しないことが望ましい。

【0027】コンテンツ送信手段17は、通信ネットワーク30を介して利用者からコンテンツ配信要求があったとき、当該利用者を認証して、コンテンツ格納手段13から、当該利用者が要求するコンテンツの、適当な複製識別子が付加された複製を、選択して読み出して、当該利用者に送信するとともに、その複製コンテンツに付加された複製識別子と、当該利用者を識別する利用者識別子とを、組として配信記録保存手段50に記録する。複製識別子の選択は、例えばランダムでよい。

【0028】利用者検出装置40では、コンテンツの権利を保護しようとする者は、識別子抽出手段41によって、記録媒体に記録されるなどによって伝送される、不正コピーの疑いのあるコンテンツ1から、複製識別子を取り出し、さらに、その複製識別子によって、利用者照合手段42において、配信記録保存手段50内の配信記録を参照して、その複製識別子が付加された複製コンテンツが配信された利用者（一人または複数、存在する）を識別する利用者識別子を検出する。

【0029】したがって、この実施形態によれば、不正コピーの疑いのある利用者を検出し、絞り込むことができる。さらに、この実施形態では、コンテンツ配信時には、複製識別子をランダムに選択して、複製識別子が付加された複製コンテンツを利用者に送信すればよいので、第1の実施形態に比べてコンテンツ配信サーバ10の負荷が軽くなる。

【0030】（他の例）コンテンツ配信サーバ10のコンテンツ送信手段17では、コンテンツ配信要求をした利用機器20を認証して、当該利用機器20を識別する利用機器識別子と、送信された複製コンテンツに付加された複製識別子とを、組として配信記録保存手段50に記録し、利用者検出装置40の利用者照合手段42では、その配信記録から、不正コピーに関与した疑いのある利用機器を検出するように構成してもよい。

【0031】特に、コンテンツ送信手段17では、明示的な認証を行わずに、各複製コンテンツを特定の何人かの利用者が復号できる鍵で暗号化して送信するとともに、その複製識別子と対応させて一つ以上の利用者識別子または利用機器識別子を配信記録保存手段50に記録するように構成することができる。この場合には、マルチキャストまたはブロードキャストと組み合わせることによって、各利用者または各利用機器を個別に認証して複製コンテンツを個別に送信する場合に比べて、伝送帯域幅を小さくすることができる。

【0032】また、上述した例は、あらかじめコンテンツを複製し、その複製コンテンツに複製識別子を割り当て、付加する場合であるが、コンテンツ配信時に、コンテンツ格納手段13から読み出したコンテンツに適宜、複製識別子を割り当て、付加するように構成してもよい。

【0033】【第3の実施形態…図3】図3は、この発明のコンテンツ配信システムの第3の実施形態を示す。

【0034】この実施形態では、コンテンツ配信サーバ10は、図2に示した第2の実施形態のそれと同じ構成とし、利用者検出装置40は、第2の実施形態のそれに對して、さらに出現頻度算出手段43が付加されたものとして構成する。

【0035】すなわち、この実施形態では、利用者検出装置40の識別子抽出手段41、利用者照合手段42および配信記録保存手段50によって、第2の実施形態と同様に、それぞれ記録媒体に記録されるなどによって伝送される、不正コピーの疑いのあるコンテンツ1a, 1b…の元になった複製コンテンツが配信された利用者を識別する利用者識別子が検出される。

【0036】さらに、この実施形態では、出現頻度算出手段43によって、利用者照合手段42から出力された利用者識別子につき、出現頻度（度数）を算出し、利用者識別子と並べてリストアップする。出現頻度の高い利用者識別子（利用者）ほど、不正コピーの疑いが大きい

と言うことができる。

【0037】これによって、コンテンツの権利を保護しようとする者は、不正コピーの疑いが大きい利用者に対して、警告を行うなどの、しかるべき措置を取ることができる。

【0038】この実施形態によれば、不正コピーの元になった複製コンテンツの配信先が複数存在する場合に、第2の実施形態に比べて、より不正コピーの疑いのある利用者を絞り込むことができる。

【0039】この実施形態でも、第2の実施形態の他の例で示したような各種の変形を行うことができる。

【0040】〔第4の実施形態…図4〕図4は、この発明のコンテンツ配信システムの第4の実施形態を示す。

【0041】この実施形態では、コンテンツ配信サーバ10は、図2および図3に示した第2および第3の実施形態のそれと同じ構成とし、利用者検出装置40は、第3の実施形態のそれに対して、さらに疑惑利用者検出手段44が付加されたものとして構成する。

【0042】すなわち、この実施形態では、利用者検出装置40の識別子抽出手段41、利用者照合手段42、出現頻度算出手段43および配信記録保存手段50によって、第3の実施形態と同様に、不正コピーの疑いのあるコンテンツ1a、1b…の元になった複製コンテンツが配信された利用者を識別する利用者識別子の出現頻度が算出され、利用者識別子と並べてリストアップされる。

【0043】さらに、この実施形態では、疑惑利用者検出手段44によって、出現頻度算出手段43から出力された、利用者識別子と出現頻度のリストから、出現頻度が定められた値（度数）以上の利用者識別子が示す利用者を、疑惑利用者として検出し、リストアップする。

【0044】この実施形態によれば、第3の実施形態と同様に、不正コピーの元になった複製コンテンツの配信先が複数存在する場合に、より不正コピーの疑いのある利用者を絞り込むことができる。

【0045】この実施形態でも、第2の実施形態の他の例で示したような各種の変形を行うことができる。

【0046】〔第5の実施形態…図5〕図5は、この発明のコンテンツ配信システムの第5の実施形態を示す。

【0047】この実施形態では、コンテンツ配信サーバ10は、図2～図4に示した第2～第4の実施形態のそれに対して、疑惑利用者リスト記憶手段19が付加されたものとして構成し、利用者検出装置40は、第4の実施形態のそれと同じ構成とする。

【0048】この実施形態では、利用者検出装置40の疑惑利用者検出手段44によって、第4の実施形態で上述したように疑惑利用者としてリストアップされた利用者を識別する利用者識別子を、コンテンツ配信サーバ10の疑惑利用者リスト記憶手段19に随時書き込む。

【0049】コンテンツ配信サーバ10では、各利用者

の専用の複製コンテンツ、すなわち当該利用者を識別する利用者識別子を含むウォーターマークが付加された複製コンテンツを、あらかじめ、コンテンツ作成手段11およびウォーターマーク付加手段12で生成して、コンテンツ格納手段13に用意し、またはコンテンツ配信時に、コンテンツ作成手段11およびウォーターマーク付加手段12で生成して、コンテンツ格納手段13に格納し、コンテンツ送信手段17は、コンテンツ配信時、疑惑利用者リスト記憶手段19を参照して、これに疑惑利用者としてリストアップされている利用者に複製コンテンツを配信する。

【0050】これによって、以後、当該複製コンテンツの不正コピーが発見された場合には、不正利用者を一意に特定することができる証拠を獲得し、または増やすことができる。

【0051】図6は、図5に示した第5の実施形態におけるコンテンツ配信処理ルーチンの一例を示す。この例のコンテンツ配信処理ルーチン70では、まずステップ20で、利用者からコンテンツ配信要求があるか否かを判断し、配信要求があったときには、ステップ72に進んで、当該利用者を認証し、さらにステップ73に進んで、当該利用者が、疑惑利用者リスト記憶手段19に記憶された疑惑利用者リストに、疑惑利用者としてリストアップされているか否かを判断する。

【0052】当該利用者が疑惑利用者としてリストアップされていないときには、ステップ73からステップ74に進んで、当該利用者が要求するコンテンツの、適当な複製識別子を含むウォーターマークが付加された複製を、当該利用者に送信し、さらにステップ75に進んで、当該利用者を識別する利用者識別子と、送信した複製コンテンツに付加された複製識別子とを、組として配信記録保存手段50に記録する。

【0053】一方、当該利用者が疑惑利用者としてリストアップされているときには、ステップ73からステップ76に進んで、当該利用者の専用の複製コンテンツを、当該利用者に送信する。

【0054】この実施形態でも、第2の実施形態の他の例で示したような各種の変形を行うことができる。

【0055】

【発明の効果】上述したように、この発明によれば、利用者側でコンテンツが不正にコピーされた場合、コンテンツの権利を保護しようとする者は、不正コピーに関与した利用者または利用機器を推定または特定することができ、これによって、当該の利用者または利用機器に対して、警告を発し、損害賠償を求める、またはリボーカ（権利剥奪）の措置を講じるなどの手段を取ることが可能となる。

【図面の簡単な説明】

【図1】この発明のコンテンツ配信システムの第1の実

施形態を示す図である。

【図2】この発明のコンテンツ配信システムの第2の実施形態を示す図である。

【図3】この発明のコンテンツ配信システムの第3の実施形態を示す図である。

【図4】この発明のコンテンツ配信システムの第4の実施形態を示す図である。

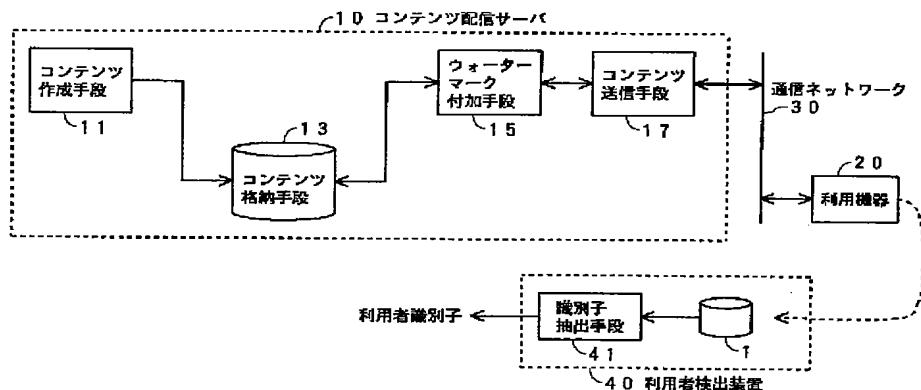
【図5】この発明のコンテンツ配信システムの第5の実施形態を示す図である。

【図6】第5の実施形態におけるコンテンツ配信処理ルーチンの一例を示す図である。

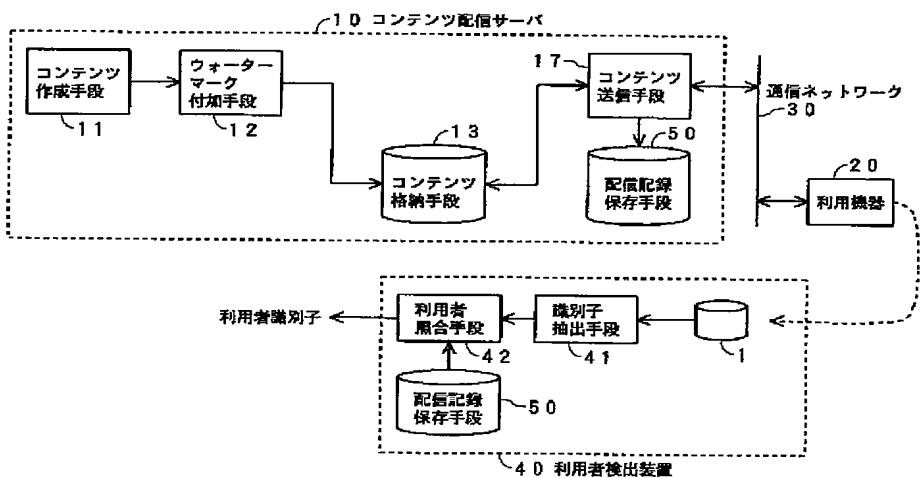
【符号の説明】

主要部については図中に全て記述したので、ここでは省略する。

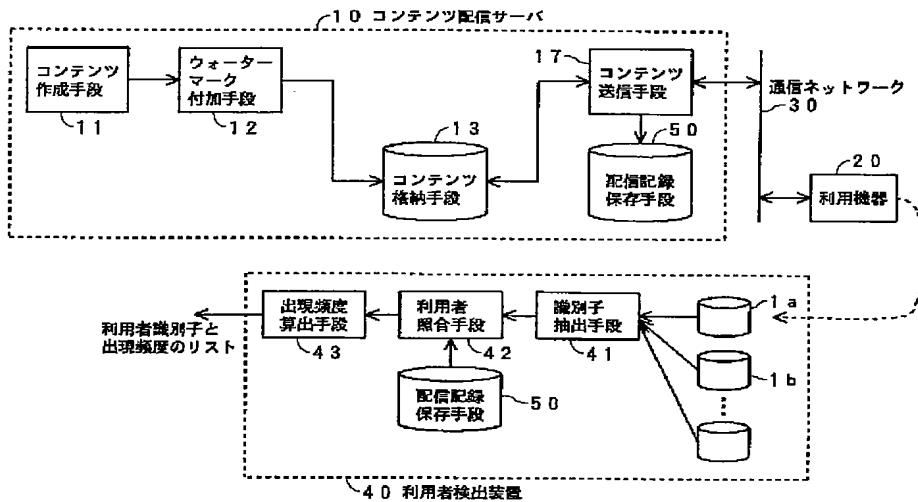
【図1】



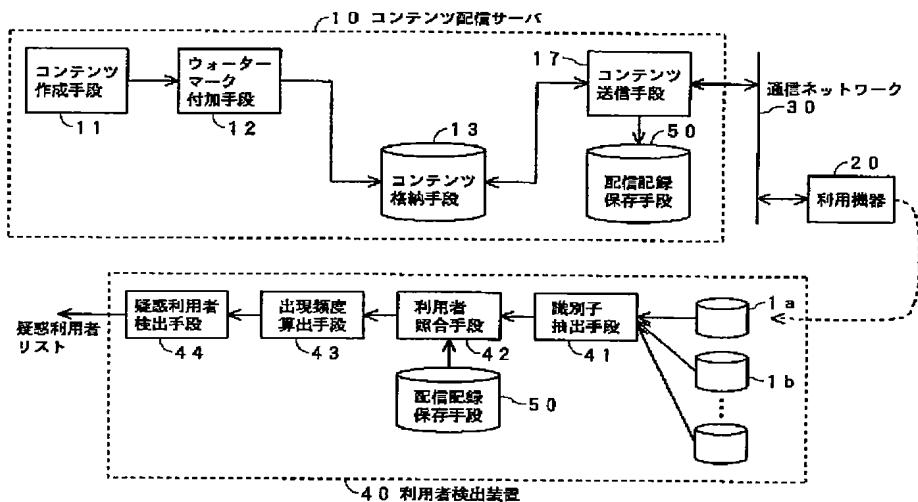
【図2】



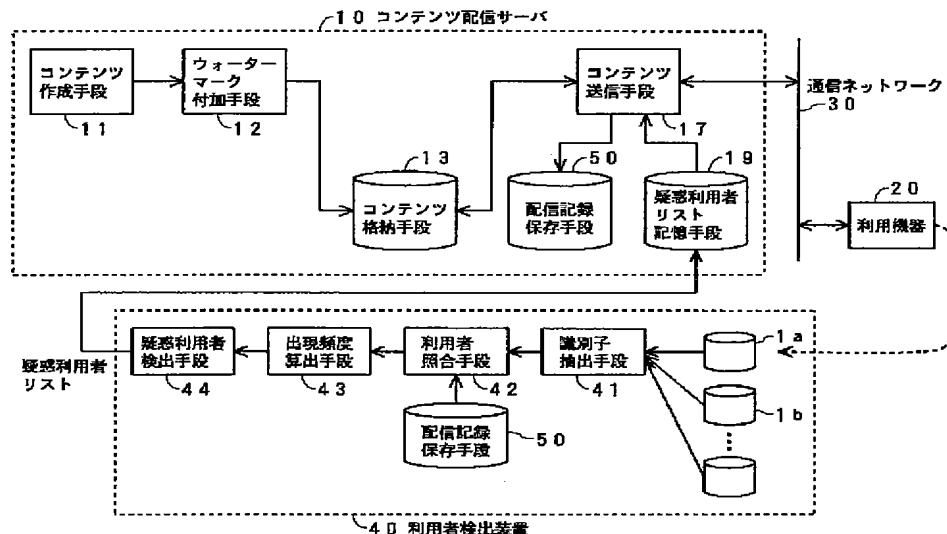
【図3】



【図4】



【図5】



[図6]

7.0 コンテンツ配信処理ルーチン

